Protection Profile for Virtualization Extended Package
Client Virtualization

Version: 1.0
2016-11-17
National Information Assurance Partnership

Revision History

Version	Date	Comment
v1.0	2016-11-17	Initial publication

Table of Contents

1 Introduction

1.1 Overview

The scope of this Extended Package (EP) is to describe the security functionality of a Client Virtualization product in terms of [CC] and to define functional and assurance requirements for such products. This EP is not complete in itself, but rather extends the Protection Profile for Virtualization (Base Virtualization PP). This is because Client Virtualization is a specific type of Virtualization System and is expected to implement security functionality that is not common to all Virtualization Systems in general. Therefore, additional SFRs have been defined in this EP to define security functionality that is unique to this particular type of Virtualization System.

1.2 Terms

All relevant terminology for this EP are defined in the Base Virtualization PP.

1.3 Compliant Targets of Evaluation

Client Virtualization, for the purposes of this EP, refers to a Virtualization System that implements virtualized hardware components locally on an endpoint machine. Endpoints are typically client hardware such as desktop or laptop computers that a user interacts with directly, but may also include headless embedded systems without direct human interaction. A Virtualization System creates a virtualized hardware environment for each instance of a guest operating system (a virtual machine) permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. Client virtualization is generally used on endpoint systems, making use of the local machine's resources (memory, CPU, etc.) to provide isolated user environments. This document does not address virtualization on mobile devices (typically devices that use a baseband processor and/or connect to a cellular network), nor does it address application virtualization or containers.

1.3.1 TOE Boundary

The TOE boundary is the same as that which is defined for a Virtualization System in general. Refer to the Base Virtualization PP for an outline of the TOE boundary.

1.4 Use Cases

Requirements in this EP are designed to address the security problem in the following use cases. The description of these use cases provides instructions for how the TOE and its Operational Environment should be made to support the functionality required by this EP.

[USE CASE 1] Locally Managed Client

> A local administrator creates and runs one or more VMs locally. This client could be stand-alone or connected to a network.

[USE CASE 2] Enterprise Managed Client

> An enterprise administrator for the VS centrally manages one or more client hypervisors, creating and configuring VMs which are then pushed to the clients. These VMs are then available for users on that client to run using the computing resources of that client. (Note that this is not Virtual Desktop Infrastructure where the hypervisors and the VMs run on remote servers. While both can be centrally managed and accessed from clients, for client virtualization, the VMs are local to the endpoint machine.)

[USE CASE 3] Headless Client

> A VM is used by a program without direct human interaction.

The use case(s) that are applicable to the TOE may influence the selections and assignments made for certain requirements in both this EP and in the base PP. For example, a locally managed client (use case 1) may not necessarily provide remote administration which would exempt it from claiming the selection-based requirement FTP_TRP.1 in the base PP.

2 Conformance Claims

Conformance Statement

A product must be evaluated against the Client Virtualization EP in conjunction with the base Virtualization PP; a product may not be evaluated solely against the Client Virtualization EP. To be conformant to this EP, an ST must demonstrate Exact Conformance, a subset of Strict Conformance as defined in [CC] Part 1 (ASE_CCL). The ST must include all components in this EP that are:

- Unconditional (which are always required)
- Selection-based (which are required when certain selections are chosen in the unconditional requirements)

and may include components that are

- Optional
- Objective.

Unconditional requirements are found in the main body of the document (Section 5), while appendices contain the selection-based, optional, and objective requirements. The ST may iterate any of these components but it must not introduce any additional component (e.g., from CC Part 2 or 3) that is not defined in the Base Virtualization PP (which this EP extends), or in this EP itself.

CC Conformance Claims

This EP is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 4 [CC].

PP Claim

This EP does not claim conformance to any Protection Profile. Note that this EP extends the Base Virtualization PP, which means that it relies on this PP to provide some set of 'base' functionality which is then expanded upon by this EP. This however does not imply that the EP itself is conformant to this PP.

Package Claim

This EP does not claim conformance to any packages.

3 Security Problem Description

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

Note that as an EP of the Base Virtualization PP, all threats, assumptions, and OSPs defined in the base PP will also apply to a TOE unless otherwise specified, depending on which of the base PPs it extends. The Security Functional Requirements defined in this EP will mitigate the threats that are defined in the EP but may also mitigate some threats defined in the base PPs in more comprehensive detail due to the specific capabilities provided by a Client Virtualization System.

3.1 Threats

This PP defines no additional threats beyond those defined in the Base Virtualization PP. Note however that the SFRs defined in this EP will assist in the mitigation of the T.UNAUTHORIZED_UPDATE and T.UNAUTHORIZED_ACCESS threats defined in that PP.

3.2 Assumptions

This PP defines no additional assumptions beyond those defined in the Base Virtualization PP.

3.3 Organizational Security Policies

This PP defines no additional OSPs beyond those defined in the Base Virtualization PP.

4 Security Objectives

4.1 Security Objectives for the TOE

This PP defines no additional TOE security objectives beyond those defined in the Base Virtualization PP. Note however that the SFRs defined in this EP will assist in the enforcement of the O.VMM_INTEGRITY and O.MANAGEMENT_ACCESS objectives defined in that PP.

4.2 Security Objectives for the Operational Environment

Because this EP does not define any additional assumptions or organizational security policies, there are no additional security objectives for the Operational Environment to satisfy.

4.3 Security Objectives Rationale

This section is not applicable to this EP because no additional security objectives are defined.

5 Security Requirements

5.1 Base PP Security Functional Requirements Direction

The Base Virtualization PP defines requirements for generic virtualization systems, not all of which provide Client Virtualization functionality. Therefore, the SFRs defined in the base PP provide the ST author with a number of selections and assignments as well as optional and selection-based requirements in order to capture the entire set of virtualization systems that can be evaluated. This section provides the ST author with specific instructions that must be taken for including the relevant SFRs from the base PP when the TOE claims conformance to this EP in particular.

At this time, there are no specific actions that must be taken with the base PP SFRs beyond ensuring that all mandatory SFRs are present, all selections and assignments are completed appropriately, and all selection-based SFRs are claimed based on the selections that are chosen.

5.2 TOE Security Functional Requirements

The Security Functional Requirements (SFRs) included in this section are those that the TSF is expected to satisfy.

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*, with additional extended functional components.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized text*;
- Refinement made by EP author: Indicated with **bold text**;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined text*;
- Iteration: Indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration, e.g., '/CDR' for an SFR relating to call detail records;
- Extended SFRs: identified by having a label "EXT" after the SFR name.

5.2.1 Security Management (FMT)

FMT_MOF_EXT.1 Management of Security Functions Behavior

FMT_MOF_EXT.1.1 The TSF shall be capable of supporting [selection: local, remote] administration.

Application Note: *Selection of "remote" requires the selection-based requirement FTP_TRP.1 defined in the base PP to be included in the ST.*

FMT_MOF_EXT.1.2 The TSF shall be capable of performing the following management functions, controlled by an Administrator or User as shown in Table 1, based on the following key:

X = Mandatory (TOE must provide that function to that role)

O = Optional (TOE may or may not provide that function to that role)

N = Not Permitted (TOE must not provide that function to that role)

S = Selection-Based (TOE must provide that function to that role if the TOE claims a particular selection-based SFR)

Number	**Function**	**Administrator**	**User**	**Notes (all SFR references are from the Base Virtualization PP)**
1	Ability to update the Virtualization System	X	N	See FPT_TUD_EXT.1
2	Ability to configure Administrator password policy as defined in FIA_PMG_EXT.1	S	N	Must be selected if ST includes FIA_PMG_EXT.1.
3	Ability to create, configure and delete VMs	X	O	
4	Ability to set default initial VM configurations	X	O	
5	Ability to configure virtual networks including VM	X	O	See FDP_VNC_EXT.1
6	Ability to configure and manage the audit system and audit data	X	N	
7	Ability to configure VM access to physical devices	X	O	
8	Ability to configure inter-VM data sharing	X	O	See FDP_VMS_EXT.1 and FMT_MSA_EXT.1
9	Ability to enable/disable VM access to Hypercall functions	X	O	See FPT_HCL_EXT.1
10	Ability to configure removable media policy	X	O	See FPT_RDM_EXT.1
11	Ability to configure the cryptographic functionality	O	O	
12	Ability to change default authorization factors	X	N	
13	Ability to enable/disable screen lock	O	O	
14	Ability to configure screen lock inactivity timeout	O	O	
15	Ability to configure remote connection inactivity timeout	X	N	
16	Ability to configure lockout policy for unsuccessful authentication attempts through [**selection**: *timeouts between attempts*, *limiting number of attempts during a time period*]	X	N	See FIA_AFL_EXT.1
17	Ability to configure name/address of directory server to bind with	X	O	

18	Ability to configure name/address of audit/logging server to which to send audit/logging records	X	N	
19	Ability to configure name/address of network time server	X	O	
20	Ability to configure banner	X	N	See FTA_TAB.1
21	Ability to connect/disconnect removable devices to/from a VM	O	O	
22	Ability to start a VM	O	O	
23	Ability to stop/halt a VM	O	O	
24	Ability to checkpoint a VM	O	O	
25	Ability to suspend a VM	O	O	
26	Ability to resume a VM	O	O	

Table 1 – Client Virtualization Management Functions

Application Note: *It is unlikely that this table will be identified as "Table 1" in the ST. The ST author is permitted to apply a refinement operation to the table name in order to give it an appropriate identification. The ST author is expected to update this table with an indication as to whether any of the 'optional' or 'selection-based' functions are included as part of the TOE. The ST author may also omit the 'Notes' column as it is provided in this EP as an aid to the ST author in constructing this table.*

This SFR addresses the roles of the CC Part 2 SFRs FMT_MOF.1, FMT_SMF.1, and FMT_SMR.2.

Administration is considered "local" if the Administrator is physically present at the machine on which the VS is installed.

Administration is considered "remote" if communications between the Administrator and the Management Subsystem travel on a network.

There is no requirement to authenticate Users of the Virtualization System. Users that have access to VMs but not to the Management Subsystem need not authenticate to the Virtualization System in order to use Guest VMs. Requirements for authentication of VM users is determined by the policies of the domains running within the Guest VMs.

For a VS where the OS is part of the platform and not part of the TOE, it is acceptable for the VS to invoke the Host OS screen lock.

Assurance Activity
The evaluator shall examine the TSS and Operational Guidance to ensure that it describes which security management functions require Administrator privilege and the actions associated with each management function. The evaluator shall verify that for each management function and role specified in Table 1, the defined role is able to perform all mandatory functions as well as all optional or selection-based functions claimed in the ST.

The evaluator shall examine the Operational Guidance to ensure that it describes how the Administrator and/or User are able to perform each management function that the ST claims the TOE supports.

The evaluator shall verify for each claimed management function that the Operational Guidance is sufficiently detailed to allow the function to be performed and that the function can be performed by the role(s) that are authorized to do so.

The evaluator shall also verify for each claimed management function that if the TOE claims not to provide a particular role with access to the function, then it is not possible to access the TOE as that role and perform that function.

5.3 TOE Security Assurance Requirements

The Base Virtualization PP lists the Security Assurance Requirements (SARs) from Part 3 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*. As an EP of the Base Virtualization PP, this EP does not prescribe any SARs beyond those defined in the base PP. The evaluator shall ensure that the SARs defined in the claimed base PP are assessed against the entire TSF as appropriate.

A. Optional Requirements

As indicated in Section 2, the baseline requirements (those that must be performed by the TOE) are contained in the body of this EP. Additionally, there are three other types of requirements specified in Appendix A, Appendix B, and Appendix C. The first type (in this Appendix) are requirements that can be included in the ST, but are not required in order for a TOE to claim conformance to this EP. The second type (in Appendix B) are requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C) are components that are not required in order to conform to this EP, but will be included in the baseline requirements in future versions of this EP, so adoption by vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

Currently, no optional requirements specific to this product type have been identified.

B. Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of the EP. There are additional requirements based on selections in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

Currently, no selection-based requirements specific to this product type have been identified.

C. Objective Requirements

This Annex includes requirements that specify security functionality which also addresses threats. The requirements are not currently mandated in the body of this EP as they describe security functionality not yet widely available in commercial technology. However, these requirements may be included in the ST such that the TOE is still conformant to this EP, and it is expected that they be included as soon as possible.

Currently, no objective requirements specific to this product type have been identified.

D. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the ‘Entropy Documentation and Assessment’ section of the Base Virtualization PP. As with other base PP requirements, the only additional requirement is that the entropy documentation also applies to the specific Client Virtualization capabilities of the TOE in addition to the functionality required by the base PP.

E. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012 • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
[Base Virtualization PP]	• Protection Profile for Virtualization, Version: 1.0, 2016-11-17

F. Acronyms

All relevant acronyms for this EP are defined in the Base Virtualization PP.